

# Forensic Times

**Berenfeld, Spritzer, Shechter & Sheer**

CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS

## “But how much data is there?”

One of the most frequent questions we receive is just how much data is involved in a case. This is common as many attorneys want to portray an opposing counsel's discovery demand as particularly arduous.

Obviously size is relative, but here is a quick comparison of everyday files and their corresponding sizes:

Word (DOC): 100 pgs = 5 MB  
10,000 pgs = 500 MB  
100,000 pgs = 5 GB

Excel (XLS): 50 sheets = 17.5 MB  
1000 sheets = 350 MB  
100,000 sheets = 35 GB

Email (MSG): 500 emails = 5 MB  
10,000 emails = 100 MB  
500,000 emails = 5 GB

## Introduction to Newsletter

Welcome to the January 2008 issue of our *Forensic Times* newsletter. Every quarter we feature recent developments in computer forensics and provide practical, actionable information on how to manage electronic discovery more effectively.

Our goal is to provide clients the most effective and efficient solutions to their electronic discovery needs. We have recently added a number of new CLE courses that we continue to offer at no-charge and will soon be unveiling a new series of seminars that I refer to as “training with teeth.” You will be receiving additional information regarding these courses and seminars in the near future.

We would like to thank our clients for entrusting us with their computer forensic and electronic discovery needs and look forward to serving you in the coming year.

Sincerely,



Robert D. Moody, JD CISM CISA  
Forensic Technology Partner  
Berenfeld Spritzer Shechter & Sheer LLP



Robert D. Moody

## Inside this issue

Introduction to Newsletter	1
Using Computer Forensics in Copyright Infringement Cases	1
Efforts to Adopt the New Federal Rules on E-Discovery	2
Allocated-space vs. Unallocated-space	2
Privilege, E-Mail and the Company Servers	3

## Using Computer Forensics in Copyright Infringement Cases

### Lawrence Navarro

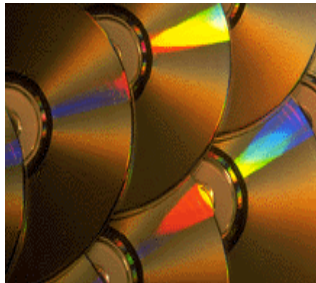
[lnavarro@bsss-cpa.com](mailto:lnavarro@bsss-cpa.com)

In a world where pirated copies of Microsoft Windows outnumber legitimate copies in some countries and software has replaced wind and steam as the main engine of commerce, the need for protection of valuable intellectual property has resulted in laws, legislation and regulations that can cause legal, non-infringing software to be seized or become the subject of a civil lawsuit.

How can a small business owner protect themselves from industry giants such as Microsoft or Hasbro? How can a company protect its proprietary software? The answer to both of these questions lies in a series of objective and subjective tests to determine whether or not two programs are “substantially similar.”

Historically, case law has shown that courts will rely on a mix of expert testimony, expert reports and demonstrations to allow the judge or jury to observe the similarity between programs. (Continued on page 4).

## Efforts to Adopt the New Federal Rules on E-Discovery



**Seth Eichenholtz**

*Seichenholtz@bsss-cpa.com*

**Arizona:** The Arizona Supreme Court has adopted E-Discovery amendments to the Arizona Rules of Civil Procedure based on the new Federal Rules. The new Arizona rules became effective January 1, 2008. See <http://www.supreme.state.az.us/rules/ramd.pdf/r-06-0034.pdf>

**Arkansas:** An amendment to the Arkansas Rules of Civil Procedure governing inadvertent production of privileged documents is under consideration. See *In re Ark. Rules of Civil Procedure, 2007 Ark. LEXIS 332* (Ark. May 25, 2007).

**District of Columbia:** The Superior Court for the District of Columbia Court is currently in the process of revising its local

rules to include the new Federal Rules.

**Illinois:** A subcommittee of the Judicial Conference is reported to be evaluating the adaptability of the new Federal Rules with recommendations collected by the Rules Committee in November 2007 and public comments set for January 2008.

**Indiana:** The Indiana Supreme Court has adopted E-Discovery Amendments largely replicating the new Federal Rules which became effective on January 1, 2008. See <http://www.in.gov/judiciary/orders/rule-amendments/2007/trial-091007.pdf>

**Maryland:** The Standing Committee on Rules of Practice and Procedure has submitted to the Court of Appeals a set of

proposed E-Discovery amendments which are similar but not identical to the new Federal Rules. See <http://www.courts.state.md.us/rules/reports/158thReport.pdf>

**Ohio:** The Supreme Court of Ohio accepted public comments on its proposed rule changes regarding E-Discovery in civil procedure through November 14, 2007. The key recommendations involved pretrial procedures, privileged documents, the requirement of both electronic and paper copies for interrogatories and requests, specifying the form of production, sanctions for failure to produce, and subpoenas for ESI from nonparties.

**Utah:** The Utah Supreme Court has approved a set of E-Discovery amendments largely based on the Federal Rules, effective November 1, 2007.

## Allocated-space vs. Unallocated-space

**A. James Boote**

*Jboote@bsss-cpa.com*

In a recent issue of *Forensic Times*, John Oakley presented an article that detailed the differences between a ghost image and forensic image. In doing so, he introduced two important terms that describe the type of space that is captured during a forensic acquisition.

The first and most familiar is “allocated-space,” which is captured by both a ghost image and a forensic image. The second term, “unallocated-space,” describes the space on a disk that is free for allocation and is generally ignored by ghost imaging.

Nearly everyone who uses a computer for day-to-day operations is familiar with allocated-space. Word documents, folders, email, programs, and all

the bits and bytes of our daily lives are stored in allocated-space. Essentially, allocated-space contains files the operating system wants to see and will present to the user.

Unallocated-space is most recognizable as the amount of storage remaining on a drive. It consists of areas of the drive that have never been written to allocated-space, the little areas at the end of computer files when they don’t quite fill their allocated-space, and areas that are left behind when active data is deleted. The deleted portion of unallocated-space is often the most interesting to investigators since it provides a wealth of data that was on the drive and deleted.

Allocated-space and unallocated-space share a give and take relationship. When a file is created, Windows finds the best

available piece of unallocated-space and writes the new file to it.

When a file is deleted, its space is marked as unallocated-space and might be overwritten when another piece of active data is created or grows in size. The deleted file’s space is not cleared or overwritten and the contents are recoverable to an extent. For example, if a user empties a smoking gun document from his recycle bin while investigators are knocking on the door to seize a computer hard-drive, analysis of unallocated-space data would produce the smoking gun document while allocated space analysis would not.

A forensic image will allow you to search computer unallocated-space for data that may have been deleted while a ghost image will not.

---

*“A forensic image will allow you to search unallocated-space for data that may have been deleted while a ghost image will not.”*

## Privilege, E-mail and the Company Servers

**Sonya Strnad**

*Holland & Knight, LLP*

When my colleagues and I review a corporate client's emails in connection with an investigation or civil lawsuit, we sometimes come across emails between one of the client's employees and the employee's personal attorney. When this happens, we look at each other quizzically and ask the question, privileged or not privileged? At first blush, one might assume that the answer is privileged because it is an attorney-client communication. Typically no one else is copied on the email, suggesting the communication was meant to be confidential. Sometimes the email is marked "highly confidential" or "privileged," or contains a generic statement at the end of the e-mail that the communication is privileged. Yet here we are, unintended recipients of the email, because the employee used the company's e-mail account to conduct personal business with his attorney. How confidential could the communication have been, and is it still privileged?

A recent case from New York State<sup>1</sup> shed some light on this issue. The court in that case held that a doctor's email communications with his personal attorney were not privileged because they were conducted through his employee email account at the hospital. But in reaching that conclusion, the court relied heavily on the hospital's email policy, which provided three relevant points:

1. the policy warned that the hospital email system should be used for business purposes only,

2. employees were on notice that there was no expectation of privacy, and
3. the company had the right to access and disclose any communications found on its system.

According to the court, the hospital's email policy diminished any expectation of confidentiality that employees might have in their hospital email accounts because it had the effect of "your employer looking over your shoulder each time you send an e-mail." This means that otherwise privileged communications are not afforded privileged status because they fail to meet the confidential communication requirement. It is worth noting that the court's decision also rested heavily on the use of the company's email server for the communication. The court distinguished other cases, in which employees used company-issued laptops to draft documents and send e-mails from their personal e-mail accounts through non-company servers. In those cases, the courts determined that the documents and emails were privileged.<sup>2</sup>

But before you log on to your AOL or Yahoo account to send an email on your company-issued computer to your personal attorney, be sure to check your company's employee handbook. In another matter, the court held that communications through a personal email account over the company-provided internet were not confidential, and therefore not privileged, because the company's policy stated that employees had no expectation of privacy in anything created, stored, received or sent over email, voice-mail or internet systems provided by the company.<sup>3</sup>

The implications of these decisions are important both for

companies, their employees, and attorneys. While many employee communications between employees and their personal attorneys do not affect the company, there may be instances in which the company and the employee have aligned interests and are both subject to the same investigation or lawsuit. In these instances, a prosecutor or other adverse party may be able to force the company or employee to hand over production of the employee's otherwise privileged communications because they were made in contravention of the company's policies, to the detriment of both the individual and the company, which may now be vicariously liable.

In light of these concerns, companies should reevaluate their email and internet policies from a risk management perspective to make sure they are properly aligned with corporate goals.

At the same time, attorneys should also be cautious about contacting clients at their company e-mail address because such communications may not be considered confidential and doing so jeopardizes the privilege of the communication.

<sup>1</sup>*Scott v. Beth Israel Medical Center*, 2007 WL 3053351 (N.Y.Sup. 2007).

<sup>2</sup>*People v. Jiang*, 33 Cal.Rptr.3d 184 (Cal. Ct. App., 2005); *Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. 2006).

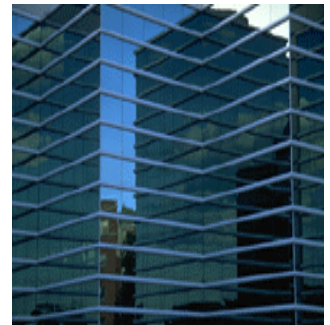
<sup>3</sup>*Long v. Marubeni America Corp.*, 2006 WL 2998671 (S.D.N.Y. 2006).

*Sonya Strnad is an attorney at the Miami office of Holland & Knight LLP, where she practices in the securities litigation and e-discovery sections. Ms. Strnad can be reached at 305-789-7618 or [sonya.strnad@hklaw.com](mailto:sonya.strnad@hklaw.com).*

*The author wishes to thank her Holland & Knight colleague, Stephen Warren, for his editorial assistance.*

---

*"Companies should re-evaluate their email and internet policies from a risk management perspective..."*



2525 Ponce de Leon Boulevard  
Suite 500  
Coral Gables, FL 33134

401 East Las Olas Boulevard  
Suite 1090  
Ft. Lauderdale, FL 33301

1551 Sawgrass Corporate Parkway  
Suite 130  
Sunrise, FL 33323

Website: [www.bsss-cpa.com](http://www.bsss-cpa.com)

Ralph MacNamara, Editor  
[Rmacnamara@bsss-cpa.com](mailto:Rmacnamara@bsss-cpa.com)

**Berenfeld Spritzer Shechter & Sheer LLP**  
Copyright © 2008  
All Rights Reserved

## Using Computer Forensics in Copyright Infringement Cases (cont'd from page 1)

Case law has also shown that copyright law does not cover individual words or the pure function of software. For example, copyright can protect the artistic design of the buttons on a specific VCR, but not the order of the buttons or the ability to play video cassettes through their use.

When examining the similarity and differences, similar items from the programs should be identified and compared using a standard framework and grading scale. In a copyright case, there are several major categories of items that need to be examined and tested. For example, a video game can have copyrightable text, music, art, packaging and source code.

Initial tests can be simple comparisons of the game's graphical features, including game title, opening screen text, level progression, losing condi-

tions, options and configurations, instructions, additional text and title screen. These comparisons can be made by simply playing through the two games being tested and comparing them screen by screen.

Further tests must be much more detailed and complex. A computer engineer can be employed to conduct forensic comparisons of the game piece texture, game piece shape, game piece size, game board layout, game board texture and game board decorative and functional elements. Other tests may look at options and configurations screens, additional artwork or animation, music tracks and various game sounds.

An important part of the comparisons typically include a detailed analysis and comparison of the games' source code. However, obtaining a copy of the source code can prove diffi-

cult. Several options include contacting the manufacturer and US Copyright Office. However, obtaining that potentially decisive piece of information is often not possible.

If the source code is obtained, there are several levels of comparison that can be performed. The initial set of tests look at how the programs are written. For example, if the programming languages are different, the chances of a direct copy of source code from one program to another can significantly decrease. The source code's logic and path can be compared. In programming, there are many ways to achieve the same output. Methods used can be compared and flow charts can be incorporated to illustrate the areas of similarity. There are firms that will use automated methods to compare the programs and provide an expert report on the findings of the comparisons.

Once the tests have been performed, the findings are compiled into a report that contains all the information required to compare the degree of similarity between the two programs. The conclusions reached by the report should be repeatable by anyone who is holding the report, the programs or both.

When comparing something as complex as productivity software or video games, the challenge lies not in the comparisons, but in choosing what to compare and how to compare it. Once the comparisons are made, they should be explained in a language that is clear and understandable by anyone.

When choosing an expert to perform the comparisons, keep in mind that the best set of comparisons, tests and procedures can be meaningless if they are not communicated properly.